UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/457,914	12/10/1999	GERMANO CARONNI	06502.0289	8208

60667 7590 06/05/2006

SUN MICROSYSTEMS/FINNEGAN, HENDERSON LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/457,914	CARONNI ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5,7-11,13-20,22,24-31,33-37,39 and 41-48* is/are pending in the application.

4a) Of the above claim(s) *4, 6, 12, 21, 23, 32, 38, and 40* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, 5, 7-11, 13-20, 22, 24-31, 33-37, 39, and 41-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4/11/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-3, 5, 7-11, 13-20, 22, 24-31, 33-37, 39, and 41-48 are pending. Claims are 4, 6, 12, 21, 23, 32, 38, and 40 was previously cancelled.

2. This is a Non-Final rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-3, 5, 7-11, 13-20, 22, 24-31, 33-37, 39, and 41-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Devine, et al. (US 6,606,708), and in further view of Albert, et al. (US 6,775,692).

As per claims 1, 18, and 35:

Devine, et al. teaches a method executed in a data processing system for providing communication access between a first process associated with a first

node and a second process associated with a second node, the method comprising:

sending a request from the first node **(col.8, lines 23-30 and col.13, lines 31-33)** to an administrative machine **(col.10, lines 55-59 and col.23, lines 17)** to verify a first node identification associated with the first process; **(col.8, lines 30-32 and 61-67)**

in response to the request, receiving security context information at the first node from the administrative machine, the security context information comprising a virtual address for the first node; **(col.13, lines 45-51 and col.24, lines 8-9)**

appending the security context information for the first process in a process table; **(col.9, lines 60-63, col.13, lines 60-67)**

opening a socket between the first process and the second process; and **(col.8, lines 22-26)**

transmitting a packet from the first process to the second process through the open socket **(col.26, lines 54-57)**, the packet comprising the security context information for the first process in the process table **(col.14, lines 6-11)**. However, Devine teaches transmitting a packet from the first process to the second process through the open socket but did not provide transmitting the packet without passing through the administrative machine.

Albert discloses a system and method for proxying a connection using a distributed architecture wherein a service manager attracts from forwarding agents packets that are sent by clients and transfers data between the client

and the server **(col.5, lines 1-15).** The packet processing includes routing the packet that includes having IP addresses or virtual addresses **(col.9, lines 57-58)** and corresponding port numbers **(col.8, lines 1-10)**. Albert system distributes network services to multiple network elements rather than one (server) and the user is prevented to connect to the protected machine. The user requests information form the server where only the server connects to the protected machine **(col.4, lines 6-17).** The network service application is physically located between the group of servers and clients **(col.2, lines 47-60)**, which is applicant's administrative machine because the network service application is a physical node that does the administrative servicing for the client to the servers. Albert provides network services without requiring a network service application to be physically placed at a node through which all incoming and outgoing packets process by a group of servers must pass and that the traffic passes through a forwarding agent **(col.7, lines 37-49)**. Further, Albert discloses the method of controlling access to a server includes sending instructions to a forwarding agent that instruct the forwarding agent to forward packets to a service manager from clients attempting to establish a client connection to the server (col.5, lines 25-32).

Therefore it would have been obvious for a person of ordinary skills in the art to modify the system of Devine with a forwarding agent so that the packet is transmitted without passing through the administrative machine as taught in Albert because this distributes the load off a single network element to multiple network elements where the user is prevented form making direct connection to

the protected machine and prevents users from direct access to protect machines (col.4, lines 15-19).

As per claims 2, 19, and36: See Devine on col.12, lines 34-37; discusses modifying a socket structure so as to accept the security context information.

As per claims 3, 20, and 37:

Devine discloses receiving the packet at the second process through the socket; **(col.8, lines 33-35)**

verifying the security context information received in the packet; and **(col.11, line 41 thru col.12, line 12)**

permitting use of the packet if the security context information is verified. **(col.9, lines 24-26)**

As per claims 5, 22, and 39: See Devine on col.27, line 43 thru col.28, line 5; discusses comparing the security context information in the received packet and security context information in another process table.

As per claims 7, 24, and 41: See Devine on col.20, lines 53-63 and col.22, lines 25-30; discusses determining whether the first and second process belong to two different linked channels ; and permitting use of the packet when the different channels are linked. **(col.23, lines 7-11)**

As per claims 8, 25, and 42: See Devine on col.24, line 2 and col.26, lines 40-42; discusses determining whether the first and second process belong to two different linked channels includes initiating a process that spawns two child processes that are connected by a shared-memory region in a memory.

As per claims 9, 26 and 43: See Devine on col.8, lines 27-28 and col.12, lines 34--37; discusses permitting use of the packet includes decrypting the packet on a node and authenticating a sender associated with the first process on the node.

As per claims 10 and 27: See Devine on col.9, lines 2-10 and col.14, lines 6-11; discusses obtaining the security context information from a third process, the security context information comprising a virtual address and a node identification.

As per claims 11, 28 and 45: See Devine on col.13, lines 31-67; discusses modifying a network stack such that the network stack requires the security context information to be present in the socket structure to transmit.

As per claim 13: See Devine on col.8, lines 52-55; discusses receiving a key that corresponds to the first node identification from the server.

As per claim 14: See Devine on col.9, lines 6-13 and col.13, lines 31-67; discusses encrypting a packet transmitted by the first process using the key; and encapsulating the encrypted packet with a header that comprises the first node identification.

As per claim 15:

Devine teaches a method of claim 1, further comprising:

sending a second request from the second node **(col.14, lines 6-35)** to the server to verify node identification; **(col.13, lines 65-67)**

receiving additional security context information comprises from the server, wherein the additional security context information includes a second virtual address for the second node; **(col.22, lines 25-30 and col.23, lines 26-28)**

creating the second process; and

appending the security context information for the second process in the process table associated with the second process. **(col.14, lines 23-30 and col.24, lines 8-14)**

As per claims 16 and 33:

Devine teaches a method executed in a data processing system for providing secure communications between a first process associated with a first node and a second process associated with a second node, comprising:

obtaining node identification comprising a virtual address from an administrative machine; **(col.10, lines 55-59 and col.23, lines 17)**

including the node identification in a field corresponding to the first process in a process table; **(col.13, line 65 thru col.14, line 2)**

transmitting a datagram that contains the node identification the first process to a socket; and **(col.13, lines 60-63)**

receiving the datagram at the second process that contains the node identification and a second virtual address **(col.22, lines 55-56 and col.23, lines 26-28)**.

However, Devine teaches receiving the datagram at the second process but did not provide e.

Albert discloses a system and method for proxying a connection using a distributed architecture wherein a service manager attracts from forwarding agents packets that are sent by clients and transfers data between the client and the server **(col.5, lines 1-15).** The packet processing includes routing the packet that includes having IP addresses or virtual addresses **(col.9, lines 57-58)** and corresponding port numbers **(col.8, lines 1-10)**. Albert system distributes network services to multiple network elements rather than one (server) and the user is prevented to connect to the protected machine. The user requests information form the server where only the server connects to the protected machine **(col.4, lines 6-17).** The network service application is physically located between the group of servers and clients **(col.2, lines 47-60)**, which is applicant's administrative machine because the network service application is a physical node that does the administrative servicing for the client to the servers. Albert provides network services without requiring a network service application to be physically placed at a node through which all incoming and outgoing packets process by a group of servers must pass and that the traffic passes through a forwarding agent **(col.7, lines 37-49)**. Further, Albert discloses the method of controlling access to a server includes sending instructions to a forwarding agent that instruct the forwarding agent to forward packets to a service manager from clients attempting to establish a client connection to the server (col.5, lines 25-32).

Therefore it would have been obvious for a person of ordinary skills in the art to modify the system of Devine with a forwarding agent so that receiving the datagram without passing through the administrative machine as taught in Albert because this distributes the load off a single network element to multiple network elements where the user is prevented form making direct connection to the protected machine and prevents users from direct access to protect machines (col.4, lines 15-19).

As per claims 17 and 34:

Devine teaches the method of claim 16, wherein obtaining a node identification further comprises:

modifying a socket structure in the socket so that the socket structure accepts the node identification; and **(col.13, lines 31-67)**

modifying a process table so that the table comprises a node identification field. **(col.23, lines 26-31 and col.26, lines 24-31)**

As per claim 29:

Devine teaches a system for placing a process executed in a node in a security context, comprising:

an administrative machine; and **(col.6, line 8-9)**

a sending node comprising:

a transmission module that transmit a request an administrative machine **(col.10, lines 55-59 and col.23, lines 17)** to verify a sending node identification **(col.8, lines 30-32 and 61-67)**, and receives security context information from the administrative machine in response to the request, wherein the security context information comprises a virtual address for the sending node; **(col.13, lines 45-51 and col.24, lines 8-9)**

memory containing a process and an associated process table; and **(col.9, lines 60-63, col.13, lines 60-67)**

an appending module that appends the received security context information **(col.9, lines 60-63, col.13, lines 60-67)** and the sending node identification for the process in the process table **(col.13, line 43 thru col.14, line 17)**, wherein the transmission module transmits a packet from the process to a receiving node **(col.26, lines 54-57)**, the packet comprising the security context information for the first process in the process table. **(col.14, lines 6-11)**

However, Devine teaches transmitting a packet from a process to a receiving node but did fails to include transmitting the packet without passing through the administrative machine.

Albert discloses a system and method for proxying a connection using a distributed architecture wherein a service manager attracts from forwarding agents packets that are sent by clients and transfers data between the client and the server **(col.5, lines 1-15).** The packet processing includes routing the packet that includes having IP addresses or virtual addresses **(col.9, lines 57-**

58) and corresponding port numbers **(col.8, lines 1-10)**. Albert system distributes network services to multiple network elements rather than one (server) and the user is prevented to connect to the protected machine. The user requests information form the server where only the server connects to the protected machine **(col.4, lines 6-17).** The network service application is physically located between the group of servers and clients **(col.2, lines 47-60)**, which is applicant's administrative machine because the network service application is a physical node that does the administrative servicing for the client to the servers. Albert provides network services without requiring a network service application to be physically placed at a node through which all incoming and outgoing packets process by a group of servers must pass and that the traffic passes through a forwarding agent **(col.7, lines 37-49)**. Further, Albert discloses the method of controlling access to a server includes sending instructions to a forwarding agent that instruct the forwarding agent to forward packets to a service manager from clients attempting to establish a client connection to the server (col.5, lines 25-32).

Therefore it would have been obvious for a person of ordinary skills in the art to modify the system of Devine with a forwarding agent so that transmitting a packet from a process to a receiving node as taught in Albert because this distributes the load off a single network element to multiple network elements where the user is prevented form making direct connection to the protected machine and prevents users from direct access to protect machines (col.4, lines 15-19).

As per claim 30: See Devine on col.8, lines 52-55; discusses the transmission module further receives a key that corresponds to the sending node identification from the administrative machine.

As per claim 31: See Devine on col.9, lines 6-13 and col.13, lines 31-67; discussing an encryption module that encrypts the packet transmitted by the process using the key; and an encapsulating module that encapsulates the encrypted packet with a header that comprises the sending node identification.

As per claim 44:

Devine teaches the computer readable medium of claim 35, wherein the appending module comprises:

an obtaining module for obtaining the security context information from a third process, the security context comprising a virtual address and a node identification; and **(col.9, lines 2-10 and col.23, lines 61-64)**

a limiting module for limiting each of the first, second and third processes to communicate with another process provided that the communicating processes share the same node identification. **(col.9, lines 2-10 and col.22, lines 25-30)**

As per claim 46: See col.8, lines 31-32 and 14, lines 23-30; discusses determining if the first and second process belong to a channel; and accepting the transmitted packet when the first and second process belong to the channel.

As per claim 47: See col.8, lines 31-32 and 14, lines 23-30; discusses means for determining if the first and second process belong to a channel; and

means for accepting the transmitted packet when the first and second process belong to the channel.

As per claim 48: See col.8, lines 31-32 and 14, lines 23-30; discusses determining module for determining if the first and second process belong to a channel; and an accepting module for accepting the transmitted packet when the first and second process belong to the channel.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100